DATE(S) ISSUED:
3/22/2011

SUBJECT:
Multiple Vulnerabilities in Apple Mac OS X Could Allow Remote Code Execution

OVERVIEW:
Multiple vulnerabilities have been identified in Apple Mac OS X and Apple Mac OS X Server. These vulnerabilities may be exploited if a user visits, or is redirected to a web page or opens a malicious file that was designed to take advantage of these vulnerabilities. Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

SYSTEMS AFFECTED:
- Apple Mac OS X Server 10.5 - 10.5.8
- Apple Mac OS X Server 10.6 - 10. 6.6
- Apple Mac OS X 10.5 - 10.5.8
- Apple Mac OS X 10.6 - 10. 6.6
- Apple Quicktime Player 7 - 7.6.9

RISK:
Government:
Large and medium government entities: **High**
Small government entities: **High**

Businesses:
Large and medium business entities: **High**
Small business entities: **High**

Universities/Schools: **High**

Home users: **High**

DESCRIPTION:
Twenty vulnerabilities have been identified in Apple Mac OS X and Mac OS X Server. These vulnerabilities may be exploited if a user visits, or is redirected to a web page or opens a malicious file that was designed to take advantage of these vulnerabilities.

The following vulnerabilities were identified by Apple:
- A denial-of-service vulnerability affects AirPort due to a divide-by-zero error.
- A remote format-string vulnerability affects AppleScript when generating dialog commands. An attacker can exploit this issue to execute arbitrary code.
- A remote heap-based buffer-overflow vulnerability affects ATS when viewing a document that contains specially crafted embedded fonts. Multiple buffer-overflow vulnerabilities affect ATS when viewing a document that contains specially crafted embedded fonts. Multiple buffer-overflow vulnerabilities affect ATS when viewing a document that contains specially crafted type

1 embedded fonts.Multiple buffer-overflow vulnerabilities affect ATS when handling SFNT tables in a document that contains specially crafted embedded fonts.

- A local information-disclosure vulnerability affects CarbonCore when dealing with applications that use the 'FSFindFolder()' function with the 'kTemporaryFolderType' flag.
- A memory-corruption vulnerability affects CoreText when viewing a document containing specially crafted embedded fonts. An attacker can exploit this issue to execute arbitrary code.
- An integer-overflow vulnerability affects HFS. A local attacker may be able to exploit this issue to read arbitrary files from a HFS, HFS+, or HFS+J file systems.
- An integer-overflow vulnerability affects ImageIO when handling a specially crafted XBM image. An attacker can exploit this issue to execute arbitrary code. CVE-2011-0181
- An integer-overflow vulnerability affects ImageIO when handling a specially crafted JPEG-encoded TIFF image. An attacker can exploit this issue to execute arbitrary code. Multiple buffer-overflow vulnerabilities affect Image RAW when handling specially crafted Canon RAW image files. An attacker can exploit these issues to execute arbitrary code.
- A security vulnerability affects the Install Helper component of Installer which may result in a service being installed on the system. A successful exploit may aid in man-in-the-middle attacks.
- A local privilege-escalation vulnerability affects the kernel due to a failure to properly check privileges in the 'i386_set_ldt' system call's handling of call gates.
- A denial-of-service vulnerability affects Libinfo due to an integer-truncation issue when handling NFS RPC packets. A remote attacker may be able to exploit this issue to cause lockd, statd, mountd, and portmap to become unresponsive.
- A memory-corruption vulnerability affects QuickLook when handling specially crafted Microsoft Excel files. An attacker can exploit this issue to execute arbitrary code.
- Multiple memory-corruption issues affect QuickTime when viewing a specially crafted 'JPEG2000' image. An attacker can exploit these issues to execute arbitrary code.
- A cross-origin information-disclosure vulnerability affects QuickTime when viewing a specially crafted website. An attacker can exploit this issue to retrieve arbitrary information across web domains.
- A remote code-execution vulnerability affects Ruby due to a integer-truncation issue in the 'BigDecimal' class. An attacker can exploit this issue to execute arbitrary code or cause denial-of-service conditions.
- An issue in Terminal may lead to a false sense of security. The problem occurs because when SSH is used in Terminal's 'New Remote Connection' dialog. SSH version 1 is selected by default.

Successful exploitation of some of these vulnerabilities could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed attempts will result in a denial-of-service.

RECOMMENDATIONS:
The following actions should be taken:
- Apply appropriate patches provided by Apple to vulnerable systems immediately after appropriate testing.
- Remind users not to download or open files from un-trusted websites.
- Remind users not to open e-mail attachments from unknown users or suspicious e-mails from trusted sources.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.

REFERENCES:

Apple:
http://www.apple.com/support/downloads/
http://www.apple.com/macosx/
http://support.apple.com/kb/HT4581

Security Focus:
http://www.securityfocus.com/bid/46950
http://www.securityfocus.com/advisories/21702

CVE:
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name= CVE-2011-0172
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name= CVE-2011-0173
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name= CVE-2011-0174
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name= CVE-2011-0175
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name= CVE-2011-0176
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name= CVE-2011-0177
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name= CVE-2011-0178
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name= CVE-2011-0179
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name= CVE-2011-0180
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name= CVE-2011-0181
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name= CVE-2011-0182
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name= CVE-2011-0183
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name= CVE-2011-0184
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name= CVE-2011-0186
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name= CVE-2011-0187
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name= CVE-2011-0188
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name= CVE-2011-0189
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name= CVE-2011-0190
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name= CVE-2011-0193
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name= CVE-2011-0194